MANAV RACHNA INTERNATIONAL UNIVERSITY

Short Synopsis

For

Ph. D. Programme 2012-13

Tracking Hybrid Intrusion Detection System in the Network

DEPARTMENT OF COMPUTER SIENCE AND ENGINEERING

FACULTY OF ENGINEERING & TECHNOLOGY

Submitted by:

Hasina A.Razzak A.Karim

Registration No.: 12/Ph.D/024

Supervisor :
Prof. S.S. Handa

Designation: Prof. CSE , FET , MRIU

Joint-Supervisor :
Dr. M V Ramana Murthy

Designation: Professor & Head, Department of Mathematics & Computer Science, University College of Science , Osmania University , Hydrabad

ABSTRACT

An intrusion detection system (IDS) is a device for providing secure data transmission or software application that monitors networks or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion detection and prevention systems (IDPS) primarily focused on identifying possible incidents, logging information about them, and reporting attempts.(IDS) is the major aspect of network computer security . Unlike firewall, it does not block particular data but keeps track of incoming data and determines whether any intrusion is underway or not. It also has records of previous attacks for future reference. IDS prevents the intrusion in first place itself. And also possibly notifies the user and brings system back on track.

As there is a rapid growth of the network applications, new kinds of network attacks are emerging endlessly. So, it is crucial to protect the networks from attackers, and it is necessary that this security concern must be articulate right from the beginning of the network design and deployment. Due to this IDS technology came into existence.

There are various problems which the existing intrusion detection system models have, such as more significant network transmission load, lower detection efficiency, and limited data process ability. Data security is a huge responsibility for sensor network as there are various ways in which security can be breached, enabling hackers to access sensitive data. Also different neural methods have been proposed in recent years for the development of intrusion detection system.

Our aim is to present an intrusion detection module based on P2P (peer – to peer) overlay networks for distributed data sharing which combines the advantages of both types of Peer-to-peer networks and minimizes their disadvantages.

Key words:

Intrusion Detection System (IDS), Hybrid Intrusion Detection System, Peer to Peer Network (*P2P),* Adaptive consistency maintenance algorithm (ACMA), Top Caching (TC) algorithm.

CONTENTS

S. No.	Description	Page No.
1	**Introduction** **1.1 Computer Network Security.** **1.2 Intrusion Detection System.** **1.3 Hybrid Peer-to-Peer System.** **1.4 Adaptive consistency maintenance algorithm.**	**1 - 3**
2	**Literature Review**	**4 - 6**
3	**Description of Broad Area/Topic** **3. 1. Core Transit Network.** **3. 2. Stub Network.** **3. 3. Idea of Hybrid Peer.** **3. 4. Consistency Algorithm.** **3. 5. Intrusion Detection System.** **3. 6. Data Base Renewing:**	**7 - 10**
4.	**Problem Identification/Objective of the Study**	**11**
5	**Methodology to be adopted**	**12**
6	**Proposed/expected outcome of the research**	**13**
7	**References**	**14 - 18**

1. **Introduction:**

The development of communication networks has been towards a better sustainability of technologies it has also raised new unwanted possibilities. Threats [Kumar et al. 2013] that were applicable only in the fixed networks are now feasible in the radio access networks. When taken into account that threats are becoming more and more sophisticated, it also means that the security systems have to become more intelligent.

The basic security measurements such as firewalls and antivirus scanners are in their limits to cope with the overgrowing number of intelligent attacks from the Internet. A solution to enhance the overall security of the networks is to increase the security layers with intrusion detection systems. Some preventive measures have to be developed to detect intrusion.

1.1 Computer Network Security:

A computer network or data network is a telecommunications network [Rai et al. 2014] which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along network links (data connections). Data is transferred in the form of packets.

Computers can be part of several different networks. Networks can also be parts of bigger networks. The local area networking a small business is usually connected to the corporate network of the larger company.

Network security [Rai et al. 2014] consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

1.2 Intrusion Detection System (IDS):

An intrusion detection system [Thukral et al. 2013] is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach goal of detecting suspicious traffic in different ways.

The goal of an intrusion detection system is to accurately detect computer security incidents, and notify network administrators. The Detection of incidents will update into the database, which will generate the default layer for the packet into the network.

There are various problems which the existing intrusion detection system models have, such as more significant network transmission load, lower detection efficiency, and limited data process ability.

1.3 Hybrid Peer-to-Peer System :

Peer-to-Peer (P2P) is a style of network in which nodes communicate to other nodes via ordinary intermediate network nodes, rather than a centralized server with full knowledge of the network so that each node performs client and server operations. Shown in figure (1).

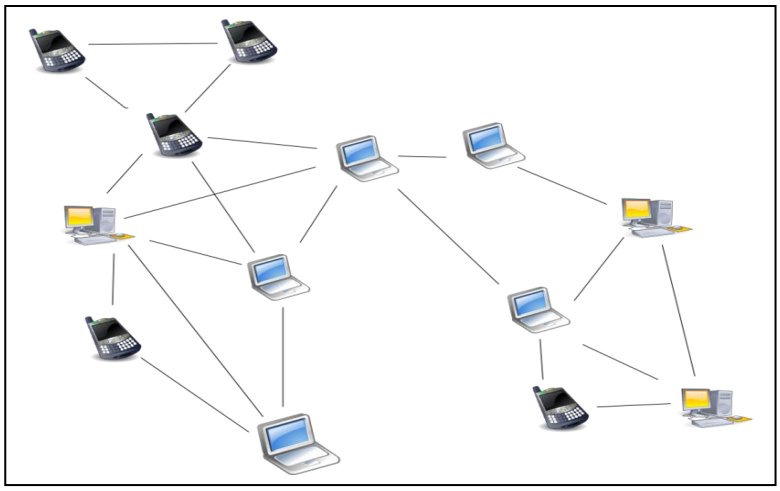

Figure (1) shows Overlay network diagram for an unstructured P2P networks.

Our work aims to presents an intrusion detection module based on P2P overlay networks. P2P overlay networks are widely used in distributed systems. P2P networks can be divided into two categories: structured P2P networks in which peers are connected by a regular topology, and unstructured P2P networks in which the topology is arbitrary.

The objective of this work will be to design a hybrid P2P system for distributed data sharing which combines the advantages of both types of P2P networks and minimizes their disadvantages. Consistency maintenance is propagating the updates from a primary file to its replica.

1.4 Adaptive consistency maintenance algorithm:

Adaptive consistency maintenance algorithm [Kalaivani et al.2012] (ACMA) maintains which periodically polls the file owner to update the file due to minimum number of replicas consistency. Top Caching (TC) algorithm helps to boost the system performance and to build a fully distributed cache for most popular information. Our caching scheme shall deliver lower query delay, better load balance and higher cache hit ratios. It effectively relieves the over-caching problems for the most popular objects.

In order to have rapid growth of the network application, new kinds of network attacks are emerging endlessly. So it is critical to protect the networks from attackers. In light of that the Intrusion detection technology becomes popular. Therefore, it is necessary that this security concern must be articulate right from detecting every new kind of attacks.

2. Literature Review :

Several and extensive review of literature in intrusion detection system have been proposed by many former researchers. In the past decade, a number of prototype peer-to-peer information retrieval systems have been developed. Unfortunately, none of these has seen widespread real-world adoption and thus, in contrast with file sharing, information retrieval is still dominated by centralized solutions. Lakshmi et.al. [2014] provide an overview of the key challenges for peer-to-peer information retrieval and the work done so far. The researchers suggested to stimulate and inspire further research to overcome these challenges. This will open the door to the development and large-scale deployment of real-world P2P information retrieval systems that rival existing centralized client-server solutions in terms of scalability, performance, user satisfaction, and freedom.(Lakshmi et.al ,2014)

In distributed systems, peer-to-peer networks are widely used. Basha et.al. [2014] proposed that since P2P can be further divided into two categories i.e., structured P2P networks in which peers are connected by a regular topology, and unstructured P2P networks in which the topology is arbitrary. Structured P2P networks usually can provide efficient and accurate services but need to spend a lot of effort in maintaining the regular topology. On the other hand unstructured P2P networks are extremely resilient to the frequent peer joining and leaving but this is usually achieved at the expense of efficiency. The main objective is to design a hybrid P2P system for distributed data sharing which combines the advantages of both types of P2P networks and minimizes their disadvantages. Consistency maintenance is propagating the updates from a primary file to its replica. Adaptive consistency maintenance algorithm (ACMA) maintains that periodically polls the file owner to update the file due to minimum number of replicas consistency overhead Is very low. Top caching algorithm helps to boost the system performance and to build a fully distributed cache for most popular information. The core structured network can narrow down the data lookup within a certain unstructured network accurately, while the unstructured networks provide a low-cost mechanism for peers to join or leave the systems freely. Basha et.al [2014] their simulation results demonstrate that the hybrid P2P system can utilize both the efficiency of structured P2P system and flexibility of the unstructured P2P network and achieve a good balance between the two types of networks. (Basha et.al ,2014) .
Elamathi et.al [2013], they stated that the research has shown that a large fraction of traffic in the Internet is occupied by peer-to-peer applications . A P2P network is a logical overlay network

on top of a physical network. Each peer corresponds to a node in the P2P network and resides in a node (host) in the physical network. All peers are of equal roles. The links between peers are logical links ,each of which corresponds to a physical path in the physical network. . All peers are of equal roles. The links between peers are logical links ,each of which corresponds to a physical path in the physical network.(Elamathi et.al,2013)**.**

Subhash et.al [2013] proposed that in a P2P network is a dispersed system in which peers utilize dispersed resources to execute a significant function in a decentralized fashion. Nodes in a P2P network usually play identical roles and these nodes are called peers. P2P networks can be divided into two categories: structured P2P networks in which peers are associated by a normal topology, and unstructured P2P networks in which the topology is random. To design a hybrid P2P system for dispersed data distribution which combines the advantages of both types of P2P networks and reduces their disadvantages is the objective of our work. Reliability preservation is propagating the updates from a primary file to its copy. Adaptive consistency maintenance algorithm (ACMA) upholds that periodically polls the file owner to update the file due to lowest number of replications reliability overhead is very low. Top Caching (TC) algorithm helps to enhance the system performance and to construct a fully dispersed cache for mostly accepted information So, researchers proposed that the caching system can deliver lesser query interruption improved load balance and higher cache hit ratios. It efficiently alleviates the over-caching problems for the most accepted objects.(Subhash et.al,2013) **.**

Data mining [J.Han, M.Kamber & A.K.Pujari 2012] (DM) refers to extracting knowledge from large amounts of data. Most of the current systems are weak at detecting attacks without generating false alarms. Intrusion detection systems (IDSs) are increasingly a key part of system defense. An intrusion can be defined as any set of actions that compromise the integrity, confidentiality or availability of a network resource (such as user accounts, file system, kernels & so on). Data mining plays a prominent role in data analysis.

Nadiammai et.al [2011] suggested data mining techniques for intrusion detection system, in their research work, the classification techniques are used to predict the severity of attacks over the network. They have compared zero R classifier, Decision table classifier & Random Forest classifier with KDDCUP 99 databases from MIT Lincoln Laboratory. Data mining is also known as knowledge discovery in databases has attained a great deal of attention in the information industry & in society. Various machine learning algorithms, for instance Neural Network, Support Vector Machine, Genetic Algorithm, Fuzzy Logic, and Data Mining have been

extensively used to detect intrusion activities both for known and unknown dynamic datasets.(Nadiammai et.al, 2011) .

In other study intrusion detection can be thought of as a classification problem where each audit record can be classified into one of a discrete set of possible categories, normal or a particular kind of intrusion. Intrusion detection using data mining have attracted more and more interests in recent years. As an important application of data mining, they aim to meliorate the great burden of analyzing huge volumes of audit data and realizing performance optimization of detection rules. Lee, W et al.(1999) described a data mining framework for adaptively building Intrusion Detection (ID) models. Data mining programs was applied to audit data to compute misuse and anomaly detection models, according to the observed behavior in the data. Amudha et.al.[2013] proposed Classification Techniques for Intrusion Detection. Classification techniques commonly used for classifying intrusion detection datasets are: Decision Trees, Bayesian Classification, Neural Network, Support Vector Machines, Associative Classification, k-Nearest Neighbor Classifiers, Rule Induction Methods. Most of these approaches directly apply standard methods to the publicly available intrusion detection datasets. Standard classification algorithms do not perform well when the computer intrusions are much rarer than normal behavior. In such scenarios, researchers have developed special algorithms and applied to intrusion detection problems. Moreover, the classification accuracy of the existing algorithms or techniques has to be improved as it is very difficult to detect new attacks. Classifier is a challenge to build an efficient intrusion detection system.(Amudha et.al,2013)

3. Description of Broad Area / Topic :

In the recent years, the evolution of a new wave of innovative network architectures labeled "peer-to-peer (P2P)" has been witnessed. A (P2P) network is a distributed system in which peers employ distributed resources to perform a critical function in a decentralized fashion.

Nodes in a P2P network normally play *equal roles*; therefore, these nodes are also called peers. The P2P participants join or leave the P2P system frequently; hence, P2P networks [Pushpalatha et al. 2014] are *dynamic* in nature. Each link in a P2P overlay corresponds to a sequence of physical links in the underlying network.

The flexibility of the overlay topology and the decentralized control of the P2P network make it suitable for distributed applications. It can also be used for distributed computing which utilizes the idle resources in the network for huge computing tasks.

Based on whether a regular topology is maintained among peers, P2P networks [Kalaivani et al. 2012] can be divided into two categories: *structured* P2P networks in which peers are connected by a regular topology, and *unstructured* P2P networks in which the network topology is arbitrary. Hence, neither structured P2P networks nor unstructured P2P networks can provide efficient, flexible, and robust service alone.

We are likely to propose a hybrid P2P system for distributed data sharing which combines the structured and unstructured P2P networks. In the proposed hybrid system, a structured ring-based core network forms the backbone of the system and multiple unstructured P2P networks are attached to the backbone and communicate with each other through the backbone. The core-structured network provides an accurate way to narrow down the queried data within a certain unstructured network, while the unstructured networks provide a low cost mechanism for peers to join or leave the system freely.

At the present time, with the network development, secured information communication is fitting more at risk because of threats [Atefi et al. 2013] from unknown sources and therefore the prerequisite for secured information assumes greater importance. Attacks on network infrastructure presently are main threats against network and information security.

With fast growth of unlawful activities in network, Intrusion Detection (ID) [Atefi et al. 2013] as a module of defense is very necessary because traditional firewall techniques cannot provide complete protection against intrusion.

For protected communication, bright analysis needs to be carried out on large volume of online data generated from the network devices. One of the popular ways of securing the network against any external threats has been that of putting in place effective IDS. An IDS is a security control or countermeasure that has the capability to detect misuse and abuse of, and unauthorized access to, network resources. An IDS, in most cases, is a dedicated device that monitors network traffic and detects malicious traffic or anomalies based on multiple criteria.

Intrusion Detection Systems [Lahre et al. 2013] is classified into 6 main types :

1. Attempted break-ins, which are detected by a typical behavior profiles or violations of security constraints.
2. Masquerade attacks, which are detected by a classic behavior profiles or violations of security constraints.
3. Penetration of the security control system, which are detected by monitoring for specific patterns of activity.
4. Leakage, which is detected by a typical use of system resources.
5. Denial of service, which is detected by a characteristic use of system resources.
6. Malicious use, which is detected by a archetypal behavior profiles, violations of security constraints, or use of special privileges.

However, we can divide the techniques of intrusion detection into two main types. They are:

1. Anomaly Detection System 2. Misuse Detection System.

Whatever the Intrusion Detection System adopted, the attackers are technically sound enough to create or develop the new kind of intrusion technique to attack on the data during transmission.

So, every emerged attacks has to get update in the System database and same kind of intrusion will not entertained for next time.

Data Mining [J.Han, M.Kamber & A.K.Pujari 2012] refers to extracting or "mining" knowledge from large amounts of data. The term is actually a misnomer. Data mining should have been more appropriately named " knowledge mining from data", which is unfortunately somewhat long. "Knowledge mining from data", which puts emphasis on mining from large amounts of data. Nevertheless, mining is a vivid term raw material. Thus, such a misnomer that carries both "data: and "mining" become a popular choice. Many terms carry a similar or slightly different meaning to data mining, such as knowledge mining from data, knowledge extraction, data/pattern analysis, data archaeology, and data dredging.

The data mining primitives specify the following:

1. The set of task-relevant data to be mined: This specifies the portion of the database or the set of data in which the user in interested. This includes the database attributes or data warehouse dimensions of interest.
2. The kind of knowledge to be used in the discovery process: This knowledge about the domain to be mined is useful for guiding the knowledge discovery process and for evaluating the patterns found. Concept hierarchies are a popular form of back ground knowledge, which allow data to be mined at multiple levels of abstraction.
3. The interestingness measures and thresholds for pattern evaluation: They may be used to guide the mining process or, after discovery, to evaluate the discovered patterns. Different kinds of knowledge may have different interestingness measures.
4. The expected representation for visualizing the discovered patterns: This refers to the form in which discovered patterns are to be displayed, which may include rules, tables, charts, graphs, decision tress and cubes.

A data mining query language can be designed to incorporate these primitives, allowing users to flexibly interact with data mining systems . Having a data mining query [J.Han, M.Kamber & A.K.Pujari 2012] language provides a foundation on which user-friendly graphical interfaces can be built.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. In accomplishing this, we divide the work into fewer modules .

3. 1. Core Transit Network:

The core transit network, called t-network, is a structured peer-to-peer network [Pushpalatha et al. 2014] , which organizes peers into a ring. We call peers in the t-network t-peers. Each t-peer is assigned a peer ID. Each t-peer maintains two pointers, which point to its successor and predecessor, respectively.

3. 2. Stub Network:

A stub network, called s-network, is a Gnutella-style unstructured P2P network [Pushpalatha et al. 2014] . The topology of an s-network is arbitrarily formed.

Each s-network is attached to a t-peer and this t-peer belongs to both the t-network and the s-network. One thing to mention about the s-network is that the topology of an s-network is a tree instead of a mesh.

3. 3. Idea of Hybrid Peer:

The basic idea behind the hybrid *P2P* system [Pushpalatha et al. 2014] is that the t-network is used to provide efficient and accurate service while the s-network is used to provide approximate best-effort service to accommodate flexibility. Peers can join either t-network or s-network directly. The hybrid system can effectively reduce the topology maintenance overhead caused by peer joining or leaving.

3. 4. Consistency Algorithm:

In the distributed data sharing, the consistency of the data needs to be focused because there are two different networks built on single. Maintaining consistency between frequently updated or even infrequently updated files and their replicas is a fundamental reliability requirement for a P2P system. P2P systems are characterized by dynamism, in which node join and leave continuously and rapidly. Moreover, replica nodes are dynamically and continuously created and deleted. For consistency maintenance, we introduce an algorithm for hybrid network, which is known as Adaptive File Consistency Algorithm (AFCA)[Pushpalatha et al. 2014]

3. 5. Intrusion Detection System:

We have many Intrusion Detection System [Pushpalatha et al. 2014] to get adopted, what ever may the IDS, and once found attack should update in the System database and provide layer to the next transmission such that the same kind of attack will not entertained. This process apparently updates the System database with all kinds of promising attacks and provides layer to the transmission of data.

3. 6. Data Base Renewing:

The process of updating the data in the database requires the knowledge of data mining, which is the key stage in the proposed system. Data Mining refers to extracting or “mining” [J.Han, M.Kamber & A.K.Pujari 2012] knowledge from large amounts of data.

4. Problem Identification / Objective of the Study:

The objective of our research work is to provide a better mechanism to improve the data transmission security in hybrid network and it can be summarized as follows:

1. To design a hybrid P2P system for distributed data sharing. It utilizes both the efficiency of the structured P2P network and the flexibility of the unstructured P2P network, and achieves a good balance between the efficiency and flexibility.
2. To design a robust hybrid P2P system for dispersed data distribution which combines the advantages of both types of P2P networks and reduces their disadvantages.
3. To maintain consistency, using file consistency algorithm for hybrid P2P system so that periodically the file owner to update the file due to number of replicas consistency overhead is very low.
4. To boost the performance of hybrid P2P, Top Caching (TCS) algorithm is used to build a fully distributed cache for popular information in P2P systems. It effectively relieves the over caching problems for the most popular objects.

It is difficult to protect the networks from attackers with new kinds of emerging attacks endlessly. As the intrusion detection technology becomes popular and efficient in finding them will not fruitful, therefore, it is necessary that this security concern must be articulate right from detecting every new kind of attacks.

5. Methodology to be adopted :

Our research work would be carried out in phases or steps to find the main objectives of the research, to study the issues related to the "TRACKING HYBRID INTRUSION DETECTION SYSTEM IN THE NETWORK" with an aim of improving the security aspects of our hybrid P2P network system by minimizing the disadvantages of the hybrid system and by proposing or developing a mechanism for better security.

Step 1: Study for the literature survey on the topic of network security system and,

Step 2: Study available tools, existing mechanisms in Intrusion Detection System and categorizing the

issues and challenges with them..

Step 3: Identify the areas of improvisation to make the Hybrid Intrusion Detection System more

secure with success achievements , and also to publish the research study and work.

Step 4: Study of various Data Mining Techniques to identifying optimal ways, for Hybrid System

in Network Security for faster Data transmission and zero packet loss through the optimization and,

Step 5: To propose or develop an improvised mechanism in a simulated environment to authenticate the

work with research paper Publications.

Step 6: Evaluation.

The over all steps in methodology used for carrying out the research work are very important to achieve our research objectives, and to develop a mechanism for better security and to improve an intrusion detection module based on P2P overlay networks for distributed data sharing

6. Proposed / Expected outcome of the Research :

The research work carried out would provide high data transmission security in P2P Network System for distributed data sharing which combines the structured and unstructured P2P networks. In the proposed hybrid system, a structured ring-based core network forms the backbone of the system and multiple unstructured P2P networks are attached to the backbone and communicate with each other through the backbone. The core-structured network provides an accurate way to narrow down the queried data within a certain unstructured network, while the unstructured networks provide a low cost mechanism for peers to join or leave the system freely.

A computer network or data network is a telecommunications network which allows computers to exchange data. So, networked computing devices pass data to each other along network links (data connections). Data is transferred in the form of packets. Network computer devices that originate, route and terminate the data are called network nodes, as shown in figure (2), which shows Overview of proposed system where nodes are communicating directly with each other.

Since network based attacks are expected to be prevalent in the future due to the mushrooming of the Internet, every capable attacks gets renewed in the database and same class of attacks will not entertained in the system during the transmission of the data.

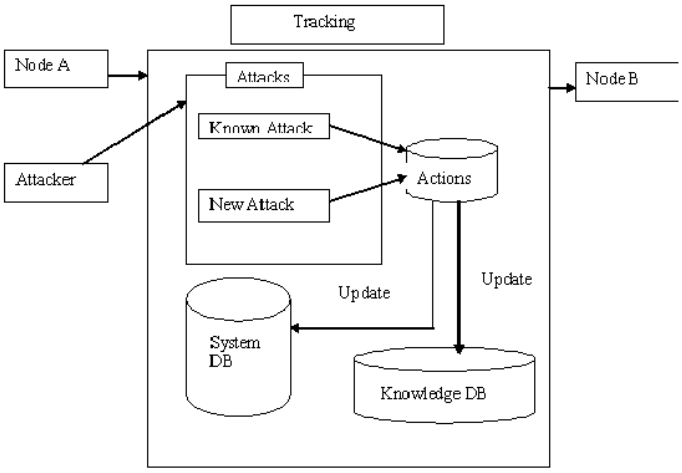

Figure (2) shows the Overview of Proposed System

7. **References:**

- A.Anand & Brajesh Patel (2012), "An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols" , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, ISSN: 2277 128X.
- A.Ismail & Aziz Barbar, "P2P Domain Classification using Decision Tree", American University of Science & Technology – AUST Alfred Naccash Avenue – Ashrafieh Beirut, Lebanon
- A.Kumar, Harish Chandra Maurya & Rahul Misra (2013), "A Research Paper on Hybrid Intrusion Detection System", International Journal of Engineering and Advanced Technology (IJEAT),ISSN: 2249 – 8958, Volume-2, Issue-4.
- A. K. Pujari (2012), "Data Mining Concepts and Techniques", Second Edition.
- Anoop & Sunil Rai (2014), "A Comparative Study of Different Types of Network", IJIRT | Volume 1 Issue 6 | ISSN : 2349-6002.
- A. Sundaram (1996), "An Introduction to Intrusion Detection" .
- A.Youssef & Ahmed Emam (2011), "Network Intrusion Detection using Data Mining and Network behavior Analysis", International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6.
- C.M.Subhash & Dr.Pasala Raja Prakasha Rao (2013), "A Well-Organized Caching System and Reliability Preservation in Hybrid P2P System". International Journal of Engineering & Science Research , IJESR/Vol-3/Issue-6/294-296.
- C.S.Lakshmi, G.sivakumar & V.Venkatachalam (2013), "Survey on Caching and Replication Algorithm for Content Distribution in Peer to Peer Network", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.3,No.5.
- D.V. Lakshmi, P.Monika Raju, A.V.L Prasuna, , M.Upendra Kumar & D.Shravani (2014), "Novel Implementation of an Efficient Caching Scheme and Consistency Maintenance in Hybrid P2P System", International Journal of P2P Network Trends and Technology (IJPTT) – Volume 4.
- E.Kalaivani & J.Selva Kumar (2012), "An Efficient Caching Scheme and Consistency Maintenance in Hybrid P2P System", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol. 2, No. 1.

- G.V. Nadiammai, S. Krishnaveni & M. Hemalatha (2011), "A Comprehensive Analysis and study in Intrusion Detection System using Data Mining Techniques", International Journal of Computer Applications (0975 – 8887), Volume 35– No.8.
- I. Stoica, Robert Morris, David Karger, M. Frans Kaashoek & Hari Balakrishnan (2001), "A Scalable Peer to peer Lookup Service for Internet Applications", SIGCOMM'01,, San Diego, California, USA. Copyright 2001 ACM 1581134118/01/0008.
- J. Han & M. Kamber (2001), "Data Mining Concepts and Techniques". First Edition.
- K. Atefi , Saadiah Yahya , Ahmad Yusri Dak, , & Arash Atefi (2013), "A Hybrid Intrusion Detection System Based on Different Machine Learning Algorithms", International Conference on Computing and Informatics, Sarawak, Malaysia. University Utara Malaysia, ICOCI.
- K. Lahre, Tarun dhar Diwan, Suresh Kumar Kashyap & Pooja Agrawa (2013), "Analyze Different approaches for IDS using KDD 99 Data Set", International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169,Volume: 1 Issue: 8.
- K. Nagaraja, Jim Pruyne, Bruno Richard, Sami Rollins & Zhichen Xu (2002), "Peer-to-Peer Computing", knagaraj @ cs. rutgers.edu, srollins @ cs.ucsb.edu.
- M. Basha, D.Arun Kumar Reddy & T. Sunil Kumar Reddy (2014), "An Adaptive Consistency and Top Caching Schemes for Distributed Data Sharing in Hybrid Peer-to-Peer Systems". International Journal of P2P Network Trends and Technology (IJPTT), V8:12-ISSN:2249-2615.
- M. R. Thakur & Sugata Sanyal, "A Multi-Dimensional approach towards Intrusion Detection System", Computer Science Department, VJTI, Mumbai, India, School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai, India.
- M.J. Freedman & Robert Morris (2002), "A Peer-to-Peer Anonymizing Network Layer", Washington, DC, USA.Copyright 2002 ACM 1-58113-612-9/02/0011.
- M. Bhatia & Sakshi Kaushal (2013), "A Hybrid Technique to Identify Peer-to-Peer Internet Traffic", International Journal of Computer Applications (0975 – 8887) Volume 74– No.13.
- M.Sazzadul Hoque, Md. Abdul Mukit & Md. Abu Naser Bikas (2012), "An Implementation of Intrusion Detection System using Genetic Algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2.

- N. Manjula, R.V. SubbaRayudu, K. Niharika & G.Prathap (2013), "Cominga Well-Organized Hiding System And Constancy Conservation In Mixture P2P System", International Journal of Computational Engineering Research||Vol, 03||Issue, 9||.
- P.B. Ambhore & Dr. Bandu B. Meshram (2014), "Intrusion Detection System for Intranet Security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, ISSN: 2277 128X.
- P.Elamathi , S.Saranya & E.Elamathi (2013), "An Efficient Hybrid Peer-to-Peer System for Distributed Data Sharing", Volume 1, Issue 1.
- "P.Amudha , S.Karthik & S.Sivakumari (2013), "Classification Techniques for Intrusion Detection – An Overview", Volume 76– No.16.
- R R. Karthick, Vipul P. Hattiwale & Balaraman Ravindran (2012), "Adaptive Network Intrusion Detection System using a Hybrid Approach", Department of Computer Science and Engineering IIT Madras, India.
- S. Sanyal, M. R. Thakur & Harshavardhan Kayarkar(2012), "A Hybrid Approach towards Intrusion Detection Based on Artificial Immune System and Soft Computing"; International Journal of Engineering Sciences and Management (IJESM), Vol. 2, Issue 2, pp. 1-8, ISSN: 2231-3273.
- S. Y. Rashida (2013), "Hybrid Architecture for Distributed Intrusion Detection System in Wireless Network", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3.
- S. Thukral , Rutba Maqsood & Divya Upadhyay (2013), "To Design an Intrusion Detection System based on Honeypot using Mobile Agent and IP Trace back Technique", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.
- S.Pushpalatha & A.V. Rama Krishna Reddy (2014), "An Efficient Caching Scheme and Consistency Maintenance in Hybrid P2P System", ISSN 2319-8885,Vol.03,Issue.33.
- S. Revathi & A. Malathi (2013) , "Network Intrusion Detection Using Hybrid Simplified Swarm Optimization Technique", International Journal of P2P Network Trends and Technology (IJPTT) – Volume 3 Issue 8.
- S. Ioannidis & Peter Marbach (2008), "On the Design of Hybrid Peer-to-Peer Systems", Annapolis, Maryland, USA. ACM 978-1-60558-005-0/08/06.

- T. Sharma & Khomlal Sinha (2011), "Intrusion Detection Systems Technology", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-2.
- V. Jaiganesh , S. Mangayarkarasi & Dr. P. Sumathi (2013), "Intrusion Detection Systems: A Survey and Analysis of Classification Techniques", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4.
- W. Tarng, Cheng-Kang Chou & Kuo-Liang Ou (2012), "A P2P Botnet Virus Detection System Based on Data Mining Algorithms", International Journal of Computer Science & Information Technology (IJCSIT) Vol 4.
- Y. B. Bhavsar & K. C.Waghmare (2013), " Intrusion Detection System Using Data Mining Technique: Support Vector Machine", International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, Volume 3, Issue 3.